BOOST
THE LEADING TRAINING PROVIDER

Internationally Certified Training Programs

PECB Certified Lead Cybersecurity Manager

Course Introduction

Organizations nowadays are affected by the ever-evolving digital landscape and constantly face new threats and complex and sophisticated cyberattacks. There is a pressing need for skilled individuals capable of effectively managing and implementing robust cybersecurity programs to counter these threats. Our Lead Cybersecurity Manager training course has been developed to address this need.

By attending the PECB Certified Lead Cybersecurity Manager, participants will learn the fundamental cybersecurity concepts, strategies, methodologies, and techniques utilized to effectively establish and manage a cybersecurity program based on the guidance of international standards and industry best practices for cybersecurity.

Additionally, this training course empowers participants to enhance their organization’s readiness and resilience against cyber threats. Participants will be well-prepared to support their organization’s ongoing cybersecurity efforts and make valuable contributions in today’s ever-evolving cybersecurity landscape.

Target Audience

This training course is intended for:

- Managers and leaders involved in cybersecurity management
- Individuals tasked with the practical implementation of cybersecurity strategies and measures
- IT and security professionals seeking to advance their careers and contribute more effectively to cybersecurity efforts
- Professionals responsible for managing cybersecurity risk and compliance within organizations

- C-suite executives playing a crucial role in decision-making processes related to cybersecurity

Learning Objectives

Upon successfully completing the training course, participants will be able to:

- Explain the fundamental concepts, strategies, methodologies, and techniques employed to implement and manage a cybersecurity program
- Explain the relationship between ISO/IEC 27032, NIST Cybersecurity Framework, and other relevant standards and frameworks
- Comprehend the operation of a cybersecurity program and its components
- Support an organization in operating, maintaining, and continually improving their cybersecurity program

Course Outline

- **01 Day One**

  Introduction to cybersecurity and initiation of a cybersecurity program implementation:

  - Training course objectives and structure
  - Standards and regulatory frameworks
  - Fundamental concepts of cybersecurity
  - Cybersecurity program
  - The organization and its context
  - Cybersecurity governance
- **02 Day Two**

Cybersecurity roles and responsibilities, risk management, and attack mechanisms:

- Cybersecurity roles and responsibilities
- Asset management
- Risk management
- Attack mechanisms

- **03 Day Three**

Cybersecurity controls, communication, and awareness and training:

- Cybersecurity controls
- Cybersecurity communication
- Awareness and training

- **04 Day Four**

Cybersecurity incident management, monitoring, and continual improvement:

- ICT readiness in business continuity
- Cybersecurity incident management
- Testing in cybersecurity
- Measuring and reporting cybersecurity performance and metrics
- Continual improvement
- Closing of the training course

- **05 Day Five**

Certification Exam

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
June 29, 2025	July 3, 2025	5 days	4250.00 $	KSA - Jeddah

FROM	TO	DURATION	FEES	LOCATION
Aug. 25, 2025	Aug. 29, 2025	5 days	4950.00 $	England - London
Oct. 27, 2025	Oct. 31, 2025	5 days	4250.00 $	UAE - Dubai